STRATEGY RESEARCH PROJECT



# UNITED STATES HOMELAND SECURITY AND NATIONAL BIOMETRIC IDENTIFICATION

BY

COLONEL PETER S. JANKER
United States Army



USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

# United States Homeland Security and National Biometric Identification

by

COL Peter S. Janker
United States
Cavalry

Professor Brian D. Moore
Project Advisor



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: COL Peter S. Janker

TITLE: United States Homeland Security and National Biometric Identification

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 32 CLASSIFICATION: Unclassified

The threat of terrorism is real. The acts of Sept 11th demonstrated that our enemy is resourceful and able to operate with ease within our homeland and among our population. The consequences of continuing to provide terrorists with the ability to operate within the United States with impunity is to welcome additional and likely more devastating attacks. The United States is currently operating in a reactive mode and must become proactive if we are to prevent further unnecessary loss of innocent lives. Our willingness to prepare for further terrorist operations by implementing appropriate biometric identification/verification systems within the United States will determine the impact and success of future terrorist acts.

Our challenge is to establish a national identification system that not only provides protection against our enemies but protects the values and respect for privacy that makes up the fabric that comprises American. In order to accomplish this we must be able to determine if our current methods of verifying identity are capable of handling the threat of terrorism. If not what steps should the Executive Branch and the Department of Defense (DoD) take to address the shortfalls? This study will attempt to answer these questions through the use of ends, ways and means analysis template to address the development of a national identification system and by identifying the role that the Department of Defense and its Biometric Management Office should play in the emerging Homeland Defense organization.

The current focus of the military, in regards to biometrics, is on itself not on American society. We can accomplish both our mission of implementing biometrics within DoD and enjoying the safe secure environment we create. Today we are ignoring DoD's role in implementing a national identification system based on biometrics. This makes DoD's mission of protecting America impossible and accepts that our nation's future identifications systems will be based upon corporate requirements. Allowing industry to establish a identification system

based upon their business model potentially threatens individual privacy and the American way of life. A suitable and effective national identification system that protects Americans while ensuring protection to American ideas is the responsibility of the Army as DoD's executive agent for biometrics.

TABLE OF CONTENTS

**IMPORTANCE OF AMERICA'S FREEDOMS AND HOMELAND SECURITY:**

> "We the People of the United States, in Order to form a more perfect Union, establish Justice, **insure domestic Tranquility, provide for the common defense, promote the general Welfare,** and **secure the Blessings of Liberty** to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."
>
> —Constitution of the United States

The preservation of every American's basic freedoms are inalienable rights that form the bedrock of what constitutes the essence of this nation. We in the military tend to focus on our role of providing for the common defense, but we are sworn to protect the entire Constitution not just compliance with a single precept. From our beginnings, the people of America have strove to attain and protect these rights for all Americans regardless of their race, religion or gender. We in the military are bound by oath to protect and defend the Constitution from all enemies foreign as well as domestic. The Department of Defense cannot accomplish its mission of protecting the Constitution without being able to identify both foreigners and citizens. The inability to identify either our enemy or ourselves brings into question DoDs ability to protect its citizens. The protection of its citizens is a critical task that every government must ensure if it is to retain the trust and confidence of its governed and hence the privilege of governing.

Today, America is arguably one of the freest nations on earth. Americans can travel at will anywhere in they wish with few restrictions. Our standard of living and economy makes America the dream of many, throughout the world, who wish prosperity on themselves and their families.

Today's immediate threats to the United States are not conventional military forces but terrorism. Terrorism as a function of its nature is not interested in engaging in direct open combat with our military, instead it seeks out and exploit weaknesses, leveraging the openness of our American society and media to gain specific insights to our vulnerabilities.

Most of the actions America has taken since September 11th have been prudent but reactive in nature. Instead of a handful of fighters protecting our airspace, we now have hundreds standing by on strip alert. We have federalized our airport baggage screeners and have tightened our security posture so tightly that even the President's security detail finds it difficult to get aboard an airliner. We cover every eventuality in our efforts to combat terrorism

but fail to base our efforts on realistic expectations of what level of effort is sustainable. American's enemies have been successful in using terrorism to negatively impact our society.

Time will go by and history has shown that our hasty and reactive security measures will fall slowly to the wayside. Not because they are bad but because they are both economically and socially unsustainable. This is not at all surprising since it is the goal of terrorism to force a opponent to try to be everywhere at all times and hence defeat himself through his own internal thrashing. The bottom line is that terrorism will strike again, perhaps even against airliners, but most definably against a target they perceive to be a weak chink in our armor.

So, what is the answer? The answer is to not become reactive to terrorism but rather become proactive. Stop attempting to plug every hole with a finger and instead step back and address the contributing cause. To hinder terrorism in the United States one must first be able to identify its own citizens as well as authorized visitors. Accomplishment of this eliminates the ability of terrorists to freely "swim" among our population. According to Sun Tzu we must "know our enemy as well as ourselves" in order to always ensure victory. The United States must have a viable national identification program. The Department of Defense is the only government agency with the capability and objectivity of implementing a program of this size and complexity. The first critical step in the process of protecting Americans is to use every mature and promising technology available. The most promising and mature field of study for national identification is biometrics.

**WHAT IS A BIOMETRIC?**

Personal identification has always been a concern. Historically identification has been relatively simple and has focused on two parameters: something you have; or something you know. Examples of something you have include having a key for a house or an identification badge permitting access to a facility. Something you know could be presenting a pin number for an ATM machine or the appropriate password when receiving a challenge on the battlefield. The world has changed with technology enabling a third factor that can be described as something you are, represented by the field of biometrics. Biometrics represents a revolutionary method of assuring the privacy rights of citizens through the accurate and timely identification of individuals without having to have identification papers or providing information such as a social security number.

Biometrics is the use of unique individual traits such as fingerprints, iris eye patterns, voice recognition, and facial recognition to identify or validate individuals. It can be as old as our recognition of the uniqueness of fingerprints as a method of identification or as new as the

use of bio-electrical signals. Biometrics are and have been in routine use for years to protect key military facilities such as chemical demilitarization sites and within certain commercial enterprises. The concept of using unique personal traits for identification purposes itself can be traced back to the payroll process used to certify that workers constructing the great pyramids of Egypt were in fact used over 4000 years ago to certify wages.[1] To the layman, biometrics may appear to be Buck Rogers technology but it is available today and its potential was recognized in this year's MIT Technology Review which named biometrics as one of the "top ten emerging technologies that will change the world." [2]

ROLE OF BIOMETRICS AND HOMELAND SECURITY

Biometrics transcend the divisions that we use to divide our elements of power: political; economical; military; and informational. Yet the DoD continues to investigate how biometrics affect the military with no regard to the effects of biometrics on the other three elements of power. This approach inherently will result in a fragmented implementation of a potentially vital tool thus failing to provide needed protection to the United States.

An old philosopher once stated "only the dead have seen the end of war." In this same light, terrorism is neither new nor will it ever cease to be a potential threat to our way of life. Historically we may find that looking back twenty years from today that September 11th was a critical wakeup call that started the process of our government recognizing the considerable scope of its responsibilities to protect all people, citizen and visitor alike, who live and travel within the United States.

The damage caused by the attack on the New York financial district was superficial by any measurement to the infrastructure of the United States, especially in comparison to the potential damage of a weapon of mass destruction of today. The risk of the terrorist attack against the financial hub of the world was not in the physical destruction that occurred but rather in ignoring its ramifications, failing to learn its lessons for today's society and implementing timely well thought out solutions.

There are those who claim that the attack against the New York financial district and its associated deadly mailing campaign has been burned into our nation's conscience, like Pearl Harbor and that we will never forget or again ever let down our guard. Yet history shows us that America has a history of forgetting its "lessons." It is one thing to state "no more Task Force Smiths," another to actually prevent another one from occurring. Many would look at the recent attacks as being unprecedented. Yet, the first bombing and combined mail attack against American's financial heart did not occur a few months ago, it occurred in the Wall Street

bombing, of September 16th 1920 and left some 40 dead and 300 injured. Before the April 1995 Oklahoma City bombing the first attack against New York's financial district was the most deadly terrorist attack in the United States. [3]

Then as now, Americans gathered by the thousands in New York to sing "the Star Spangled Banner," then as now, a recent immigrant group found itself broadly and unfairly blamed for the attacks of a few. Then as now, the attack was conducted in the heart of the financial district as an affront directly against the American people.[4] We must do all we can to ensure that we do not fail to do all we can to establish systems to help preclude such terrorist acts from again occurring in the future as we have so often failed in the past. Our strategy against terrorism must become proactive and preventive rather than reactive. We cannot afford to simply slap a band aid on a "sucking chest" wound and pray for a swift recovery, we must take comprehensive preventative actions. Any other approach risks the consequences of future attacks by terrorists using weapons of mass destruction that would not be acceptable to the American people.

The protection of privacy and the relentless encroachment of the capabilities of technology are two elements that must be controlled. This nation is hobbled with an obsolete national identification system built upon the social security number, birth certificate and driver's license. This inefficient system is changing not because of any specific action on the part of our national government but because corporate America recognizes that, the old system is broken. Industry is well on its way to creating information systems that will ensure validation of identity based upon their commercial interests.

Today, technology exists that makes it both feasible and economical to biometrically identify everyone in the United States. A remaining issue is how the data that is collected will be used. Privacy issues exist on both the data collected and the information about an individual that can be inferred. An example is that iris recognition technology can be modified to screen for recent drug use or for related sensitive medical information such as patent hypertension. Neither is necessary for protection against terrorism and both invade the privacy of individuals.[5] Down this path are unquestionable vulnerabilities of our personal freedoms and rights.

This nation can ill afford to stumble into a business "solution" to our identification and security needs like we did regarding the implementation of our current Social Security Number (SSN) and driver license based system. We must orchestrate the use of the best technology and concepts to achieve an optimal end state that protects the privacy of every individual while providing the means to make America secure.

The U.S. must cease looking at privacy and technology being diametrically opposed elements and must instead work towards synergistically blending the two in order to preserve our freedoms while protecting Americans.

## WAYS/MEANS OF BIOMETRICS

The following biometrics represents an overview of several biometric technologies currently available. The description is meant to provide a short, concise overview of several robust technologies and does not include every biometric currently available.

### FINGERPRINT

Fingerprints have long been used for accounting by the human race. Fingerprints were discovered on clay tablet seals on business transactions from ancient Babylon. Sir Francis Galton, a British anthropologist, first published his observations of fingerprint individuality and permanence in 1892 after his cousin Charles Darwin forwarded research that he found interesting.[6] A hundred years of use has proven fingerprints to be a valuable method for individual identification.

In the case of a fingerprint biometrics system, an individual is registered with a scanner, which can be as small as a pencil eraser and costs less than ten dollars, that records the individual pattern unique to each person. A template is then created that represents the location of each unique parameter and a resulting mathematical representation is generated. A subsequent validation is made when an individual provides his fingerprint for correlation to the template stored in the system. It is important to note that the image itself does not have to be stored or referenced; only the template is necessary which reduces dramatically the electronic storage needed. Having the template itself does someone attempting to circumvent security no good since it is the ability to present an original finger or biometric that begins the identification process. Technology maturity is such that "aliveness" parameters, such as blood flow, electromagnetic and blood pressure, preclude detached fingers from being effective. Fingerprint biometrics are relatively mature and commonly used to protect large scale banking transactions. Fingerprint based systems are also commonly used for door entry systems and automobile access. The technology of today is capable of being sized small enough to fit on the trigger of a weapon or embedded onto or into a credit card or identification card on either an electronic chip or magnetic strip.

Fingerprint technology is capable of being used either by itself or in conjunction with other means of identification and its capabilities and functionality continues to be enhanced. Development of appropriate tactics, techniques, and procedures are key to acceptance of this

technology by the military for future weapon systems. In certain research and development programs, prototype weapon platforms have weapon control systems whose access is already protected by fingerprint validation.

Fingerprints are currently being used in a number of civil and military applications. Countries such as Mexico have already implemented biometric systems to combat duplicate voter registration in their presidential elections and are already using biometric fingerprint technology to identify individuals within their military. Major international banking organizations use fingerprint logons to protect access to the computer systems that manage the transfer of billions of dollars.

The U.S. DoD is not asleep at the switch in regards to biometrics. Every soldier, sailor, airman and marine has his or her fingerprints biometrically registered upon enlistment into each respective service. The Defense Manpower Management Command (DMMC) collects a fingerprint suite as well as a photograph and Deoxyribonucleic Acid (DNA) sample from every individual as part of the induction into service and issuing of an identification card. Each service member's fingerprint record is then sent to the Federal Bureau of Investigation (FBI) fingerprint repository in West Virginia to be cross-checked against a known listing of criminals and wanted individuals. The new military identification card contains a fingerprint biometric that can be used for identification or for validation when operating emerging information systems.

Today, fingerprint biometric devices can be found on door knobs for room access, building access systems, built into laptop computer keyboards and on a multitude of smaller devices such as Personal Computer Memory Cards (PCMCIA), credit card sized devices and on items as small as the trigger of a rifle or pistol. The Army is currently using fingerprint biometric devices to secure access into facilities that handle classified information as well as to control access and operation of weapon systems located on experimental vehicles. U.S. Forces Korea also uses fingerprint technology to control access onto their military bases using a Defense Manpower Management Command developed software application.

FACIAL

Facial recognition systems are quickly maturing and have the unique ability to be used without the subject's knowledge and at some distance. The system itself uses key facial features such as earlobes, eye sockets, nose features, and mouth to create a unique face print template.

Since the technology does not have to use skin color, this system does not support the profiling commonly condemned by civil rights activists. A version of this technology was

recently used to hunt for terrorists at Super Bowl XXXV in Tampa, Florida.[7] While no terrorists were identified the system did identify a number of petty criminals that attended the event.[8]

The technology is also being used by various US state agencies to hunt for and identify individuals who have duplicate and false drivers licenses. It was found that many professional drivers had multiple driver licenses in order to evade the ramifications of multiple driving offenses. Cracking down on these drivers had the result in getting dangerous drivers off our nation's highways.

In Newham, England the British installed facial recognition systems in conjunction with a series of 200 cameras to fight street crime and identify terrorists. The cameras, which are located in conjunction with the transportation system, have been effective in reducing the level of criminal activity. Israel also uses the same technology to scan Palestinian workers at border checkpoints. Australia is planning on using facial recognition software to identify aircrew passports this year and will expand the scope of the biometric identification initiative to all its passports in the future.[9]

The technology is not perfect. The National Security Agency (NSA) demonstrated that state of the art live mask technology could create a "life mask" that can fool some of the systems currently being used commercially. The cost however is not inexpensive at about 45-50 thousand dollars per mask. Industry is already looking at ways of shoring up this vulnerability by coupling in infrared technology for aliveness validation.

There is extensive evaluation of this technology as part of the Defense Advance Research Projects Agency (DARPA) human ID at a distance program. Their evaluations assess the ability to use facial technology's ability to identify mugs, thugs, and terrorists operating within large groups of people such as rioters. The concept is to identify ringleaders who show up over and over again at riots. These individuals can be effectively identified and removed thus defusing sensitive mob situations.

Many DoD ID cardholders do not realize that facial biometrics are part of their current ID card. The photograph located on the front of the card is the most visible part of the individuals ID card and normally facilitates the ability of the low tech and manpower intensive method of individual checking personal identification. The three dimensional barcode on the back of the service ID card contains a digital image of the individual's face that enables the card to be machine read, thus reducing the potential for identity theft by simple photo manipulation.

IRIS

One of the most promising biometrics technologies is Iris. This biometrics uses the black and white pattern contained in the colored portion of the eye to establish an eye print. Since it uses approximately 250 points of reference, vs. the 16 or so used by fingerprints, the accuracy is incredible with a false accept rate of about 1 in every 12 million attempts.

Currently the iris systems can be used at ranges from 3 to 4 feet, but under lab conditions, identification has been done at ranges up to 30 feet. This is a very promising and mature technology and is currently being used to access selected DoD secured and classified facilities, to include the command and control facility on a U.S. Naval War ship. Britain's Immigration and Nationality Directorate is planning to introduce Iris-recognition capability on December 4th 2001 to ease the entry of persons who visit England frequently.[10] Iris recognition is a proven technology and was used successfully in the Nagano Winter Olympics to match shooters with their weapons.[11] It was also used during the Sydney Olympics on turnstiles that allowed athletes to access their venues.

Iris technology is being used today for controlling access to sensitive intelligence areas and can be used either by itself or in conjunction with other means of identification. Expansion of its use into operational systems and key weapons systems, especially those of a sensitive nature i.e., Stinger missiles and access to weapons of mass destruction, is envisioned.

Iris recognition is not intrusive and unlike many biometrics does not require users to make physical contact with a reader or device. The nature of taking a photo of the iris makes this a user-friendly technology. It is the only current biometric that has a proven capability to be used under anticipated combat conditions, specifically while masked in an Nuclear Biological and Chemical environment.

This technology is currently being used for access to offices of the Chief of Staff of the Army, within the Pentagon.

VOICE

A maturing biometric currently being used on computer networks and phone systems, voice biometric is potentially one of the most critical for the DoD. Typical applications include a commercial-off-the-shelf screen saver software application that costs less than $100 and can be installed on a personal computer within 5 minutes. The settings can then be set to lock the screen after a certain number of minutes have elapsed without any keyboard activity. The returning user then simply states his password phase and the system permits the user to continue operations. .The Army is looking at placing this software application on classified

computers used by General Officers within their homes. The use of a voice biometric allows a user to leave his terminal for a few minutes without having to log off and then go through the long process of connecting back onto the classified network.

Voice as a biometric is also being used commercially by organizations that accept orders by telephone. Verification of caller identification is critical in order to ensure that only an authorized customer is placing an order, prior to shipping costly or restrictive products out.

There are three primary issues with voice as a biometric. One is that the voice can become distorted due to several factors such as maturity change, fear, illness or hindrances such as the wearing of a protective mask. Second, the clarity and thus accuracy of voice identification depends on the input device being used. If an individual registers their voice via phone and then attempts to be verified over radio a false rejection may take place because of the difference in hardware. Third, voice identification is sensitive to background noise. Attempting to log onto a laptop computer on a commercial airliner may be difficult due to the engine background noise. Industry is working to make voice biometrics more robust.

**THE NATURE OF THE THREAT TO AMERICA**

How did September 11th happen? Just hours after the attacks we sat in front of our televisions and saw the faces of the terrorists as they went about their final preparations to commit murder. How can a nation that has such technology that we can in hindsight follow Mr. Atta, a known and wanted terrorist, from the time he enters the United States to his gaining cash from an ATM and his final boarding onto an doomed aircraft without taking some type of preventive action? How can it be that when we know the faces of suspected terrorists that we can react only by posting a photograph on a post office wall?

The ringleader for the September 11th attacks was a known terrorist by the name of Atta. If a ticket agent or security guard had recognized Mr. Atta I do not believe that anyone would argue that it would have been an invasion of Mr. Atta's privacy for authorities to arrest or detain him. Atta could have been highlighted on "America's Most Wanted" without attracting the ire of civil libertarians. Does " America's Most Wanted" represent the limitations of how we can harness technology to provide protection to America?

There has been a marked reluctance to use technology, such as biometrics, to enable national security systems. Motor vehicle officials representing the American Association of Motor Vehicle Administrators (AAMVA) are in the process of requesting 100 million dollars from Congress to create a national identification system based upon a biometrically enhanced driver's license that uses fingerprints as a unique identifier. Despite the justification of the

AAMVA that the whole issue is one of "improving public safety, protecting national security and preventing identity fraud" civil-liberties organization such as the Electronic Privacy Information Center as already claiming that such as system gives the government too much capability to monitor individual actions and is subject to being abused.[12]

Instead we must take the same reactive measures we have taken in the past. We must rely on overworked and underpaid security personnel and argue over procedural techniques and points that provide incremental if any benefit such as if airline security screeners should be civilian contractors or government employees. We emplace military police at every gate on military installations throughout the world, not to achieve a measurable increase in security but because in a crisis we fall back on tactics, techniques and procedures that we know, which is to throw manpower at a problem. In essence, we work very, very hard but not very smartly while inherently knowing that we must work hard and smart to combat terrorism successfully.

At the same time we passively accept stovepiped security systems that do not communicate and which require impossible diligence to operate. Even when local governments such as the city of Virginia Beach, Virginia approves the use of facial recognition technology it is done as a local stovepipe system without an interface to national databases of known terrorists.[13] This inability to develop useful information by linking associated data is a capability that the United States government does not have the ability to do according to Ruth David, a former deputy director for science and technology at the Central Intelligence Agency.[14] Thus stovepipe use of biometric technologies provides an environment where those who wish to do America harm can operate with impunity. DoD knows the danger of creating systems that cannot communicate. Much of our transformation costs will be to redesign our current stovepipe systems so that they can operate as a system of systems. Why then are we allowing local stovepipe identification systems to exist and to be created for what is a national identification requirement? When building an information system from the ground up it is no more costly to build an open national system than a closed local stovepiped system. Building an open system just takes leaders with vision. The acceptance of biometrics as a tool for national security is like Army Transformation, it has social, intellectual,[15] and leadership dimensions that must be addressed.

## THE DEPARTMENT OF DEFENSE'S ROLE IN NATIONAL IDENTIFICATION AND BIOMETRICS

SOCIAL AND INTELLECTUAL

Why doesn't somebody do something about the lack of an effective national identification system? The answer is not that the people of the United States do not want anything done about it. In a survey just after September 11th, 71 percent of U.S. respondents wanted a national identification system based upon biometrics, specifically both fingerprint and iris scans.[16] Cost does not appear to be a factor. The CEO of Oracle, the most respected relational database corporation in the world, has offered to provide the database structure to implement a national identification system for free. [17] The reason nobody has comprehensively addressed the lack of a national identification system is because of the same complexity of the issues that cover Army transformation.

It is not that our national leadership lacks the initiative to do what must be done. Sen. Christopher S. Bond of Missouri has confirmed that his ID-Card proposal, signed into law by President Bush, will require all foreigners to the United States to have an ID-Card that is implemented via biometrics and centralized comprehensive database of visitors and non-citizens.[18] Who is going to implement this law and how do you know if someone is should have a biometric ID-Card? Is that fact that someone is a visitor or a noncitizen stamped on ones forehead? The wording of the law enabled the political ramifications surrounding the issue of individual privacy of citizens to be ignored for the time being. In essence, politically it is too easy for leaders not to do anything about it, since the wrong action is perceived, by politicians as being like touching the live rail on a subway system...instant political death. The only organization to undertake this effort is one that the American people trust. According to recent surveys the American military and its leadership is one of the most trusted organizations in the United States.

The DoD Biometrics Management Office (BMO) was created by direction of Congress under Public Law 106-246 as the single DoD lead for biometrics. The Army is the lead service and is tasked with managing every aspect of biometrics as it relates to the military. There are two issues concerning the manner in which the office is being used. The first is that it is subordinate to the Combined Access Card program that concentrates on identification using the concept of identity being something you have instead of biometrics whose focus is something you are. The second issue is that the issue of identity is a national issue that goes outside the scope of the military. Can the military implement biometrics using their current approach?

Absolutely! They cannot however perform their primary mission of protecting America unless they change their biometric focus from internal to the military to our society as a whole.

The scope of the Public Law 106-246 does not extend to establishing a national identification system nor does it address international ramifications. As a result the DoD is unable to provide adequate Homeland Defense to American citizens against the threat of terrorism. The Department of Defense Biometric Management Office is an agency that if properly augmented and directed can manage the development of a creditable national identification system that is biometrically based.

The mission of the BMO must be expanded to include development of a centralized and biometricized national identification system under the Office of Homeland Security not only for visitors but also for all Americans. This must be a part of a comprehensive identity program that is worldwide. In essence we are talking about replacing the current passport system with one enabled via biometrics.

Can our military leadership handle this? It has only been a few months since we undertook the seemingly incredible difficult effort of transiting the Army to a new beret. Can today's officer in be flexible enough to effectively "think outside the box?" Almost sixty years ago, in the heat of battle, on the shores of Normandy with the outcome far from certain a combat commander once uttered his tactical vision statement by proclaiming, "only the dead and the dying were going to remain on the beach."[19] Given the explosive pace of today's technological revolution the same terms could be applied to leaders that ignore the implications of emerging technology such as biometrics.

LEADERSHIP:

> "The U.S. Army of the most mechanized nation on earth came to the threshold of WWII wedded to Strategy, Operational Art and Tactics deeply rooted in the 19th Century"
>
> —Edward Katzabach
> The Horse Cavalry of the 20th Century

Implementing change is one of the most difficult challenges a military officer must face if he is cursed by living during what the ancient Chinese called "interesting times." General George C. Marshall took office as the Chairman of the Joint Chiefs of Staff on 1 September 1939, the day Germany invaded Poland. On the eve of WWII General George Marshall found himself with a military anchored to its past and reluctant to change. The threat of imminent world war dictated that Marshall fire over four hundred colonels and generals, thus creating an

appropriate leadership environment to implement change. General Marshall in one swift action eliminated the entrenched resistance to do anything differently than had been done for those last thirty years. In hindsight, General Marshall took harsh but necessary action to transition from a peacetime bureaucracy to a focused fighting force. Today our challenge to harness technology change and transform the military is every bit as vital as we endeavor to secure our homeland while protecting America's freedoms.

If the Army is to be prepared to protect and defend the nation the identification and harnessing of leaders of character that can effectively operate within an environment that is rapidly changing is of strategic importance. Commanders cannot dictate transformation: they must be capable of leading it. The engine that drives change is leadership. [3] It is in the timely recognition and acceptance of the potential of technology that the military often falls short.

Military leaders with the vision necessary to see past the immaturity of a given technology are few and far between. We often not only fail to assess the technology but often also fail to forecast how the technology can be integrated into the "system." We as leaders tend to be intolerant of technology immaturity and dismiss anything that is not "ready for prime time." What we fail to grasp is that complex systems are the results of an iterative development process sometimes extending over many years. Can anyone doubt that without the World War I "pickle" tank in 1918 we would not have had the MIAI Abrams for Operation Desert Storm?

When America goes to war we must do so with our entire national industrial might. Effective military leaders must embrace technology and provide timely feedback into the iterative product improvement process. Leaders with vision must implement changes proactively rather than reactively in concert with being professionals. As professionals, unless we can manage technology and its influence on our profession we risk becoming a bureaucracy and irrelevant on the battlefield.

We as leaders must recognize the peril in falling back to comfortable "solutions" that have failed in the past. We must take calculated risks that are seeped in the knowledge gained by many battlefield "failures." We must harness technology and make it sing for us because if we do not, then our enemies will.

## WHY SHOULD THE MILITARY CONCERN ITSELF WITH THE EMERGENCE OF THE BIOMETRICS INDUSTRY?

Every commander recognizes the need to know both himself and his enemy in order to avoid peril. Today the U.S. can do neither since we cannot identify our own citizens much less potential terrorists. The United States lacks even a rudimentary national identification system to

preclude terrorists from operating in the open sea of our civilian population. It is critical that we not only use biometrics within the DoD but that we also have biometrics to aid us in protecting Americans within the aspects of Homeland Security.

Biometric technology is evolving every day. So why should the military get involved with the biometric industry while much of the technology is in the process of maturing? Why not wait until the technology is fully mature and then go in and purchase commercial-off-the-shelf (COTS) applications for the DoD?

The answer is that DoD must be involved at the ground floor of the evolution of biometrics if it wants to preclude itself from having to commit resources for its own independent biometric identification system. The BMO is working hand in hand with the National Institute of Standards and Measures to ensure that DoD requirements are incorporated into biometric data standards that focus industry's direction. We must be fully engaged because the world has changed. The DoD can no longer directly dictate where and what industry focuses its attention on. The days when we owned the data rights and could tell a contractor what programming language to use are over. However for a limited time DoD has the opportunity to influence the requirements by which biometric applications are developed. Once the market for biometrics is established DoD will lose any ability to influence the direction that biometric technology heads. The DoD cannot afford to not leverage off of commercial biometric technology and be left in the position of having to develop its own military biometric applications and tools.

The problem with the military using a pure commercial off the shelf (COTS) product is that we inevitably have some "minor" modification that would make the item perfect. The change could be as easy as changing the items color to camouflage or blue, depending on the service, or as complicated as making the system work over aster communications bandwidth. Regardless, these DoD requests for changes occur at the point where industry is least able to modify its product. This is the point where the product has already been built and in some cases the production lines are already active. By working with the biometrics industry up front we can assure that the requirements that influence the application's developments are incorporated at the point of the product's lifecycle where its is most efficient.

The idea is to benefit both the government as well as industry. We as the DoD should be willing to underwrite some of the development costs that make the application more appealing to the government as well as to the eventual commercial market. What we would have effectively accomplished is a win-win situation for all the parties concern. Thus the COTS fingerprint system that is produced by industry can also be used by DoD in a tactical environment because it utilizes a thermal light source rather than a visible light source. For a

limited time we are at a point that the DoD can influence the requirements by which the biometric industry develops products.

A ONCE IN A LIFETIME OPPORTUNITY

This is a limited opportunity. Once commercial interests come on board fulfillment of government requirements will take a back seat. One example of this is the Microsoft suite of software applications. None are as infamous as PowerPoint. The use of this application has created an entire breed of Pentagon workers known as "PowerPoint Rangers." In vain, commanders have tried to reduce the complexity and length of briefings done by these folks, not because of the lack of need to facilitate communications but because the animation and flashy background and colors eats up critical communications bandwidth. The wasteful use of bandwidth could have been avoided if DoD had worked with Microsoft years ago to ensure that PowerPoint information could be transmitted with austere communications bandwidth. Who would have won? Both Microsoft and DoD would have been better off since both could then support the emerging wireless environment that is emerging as the topology of choice. Our national strategy must be one of supporting technology that supports both commercial as well as military applications.

**WHY IS THE STATUS QUO NOT SUFFICIENT?**

It is not as if the United States does not already have a national identification system. We do, however it is broken and ineffective. The basic driver's license is standard for identification purposes throughout every state. The primary issue with the use of the driver's license is that they use technologies that are easily circumvented. Fraudulent driver licenses can and are procured by college freshmen in every university and college. On the street the issuing process for driver licenses can be circumvented for $50. In fact, two of the September 11$^{th}$ terrorists simply paid an illegal alien that sum to procure their driver's licenses. The U.S. is currently pursuing court changes against the hapless accomplice.

The use of a photograph for identity is technologically obsolete. Photographs have been used for ID cards since the middle 1800s. As early as 1930, Joseph Stalin had his enemies e.g., Trotsky, "erased" from historical photographs of the history of communism. Newsweek cosmetically "edits" photographs to make them more attractive and even an esteemed institution like the National Geographic Society has admitted to moving the Great Pyramids of Egypt so that they would esthetically line up. Our preschool children think no more of editing a photograph on their personal computer than today's terrorist does of creating false credentials.

The military is not blind to this risk concerning photographs. Every military identification card has two photographs of the owner. The physical photograph located on the front of the card and a second digital photograph is located within the two dimensional barcode located on the back of every card. Thus military identification card holders can be manually verified via a database comparison if the card is inserted into a card reader. The problem with this process is the resources it takes, specifically the time and energy for an individual to conduct a check. The labor intensiveness results in few if any identification cards being verified by card reader.

## ONGOING BIOMETRIC IMPLEMENTATIONS IN SOCIETY

Unlike other identification methods, biometric automation systems are unique since they have the potential to ensure privacy while at the same time providing security. We must ensure that our emerging identification strategies do not result in individuals losing their privacy. Freedom must be protected by both protecting American rights and protecting America. The processing power of computers makes it possible to have a technological "mother" to quickly and accurately identify each of her children. There are many concerns regarding this capability especially the risk of "big brother" knowing and seeing everything. Some even see biometrics as representing the "mark of the beast" foretold in the Bible. The problem is that the ad hoc solution for identification that we live with today is far worse, from a privacy perspective, than what could be created today.

What is happening now is that various civilian and military organizations are taking their own initiative to implement biometric "solutions" that are simply "stovepipes" using advanced technology. Virginia Beach, Virginia and Tampa, Florida are two cities that have implemented face-recognition systems to deter crime.[20] Both cities have implemented measures to ensure privacy, one by establishing an oversight committee the other by not storing faces other than those of criminals. Interesting enough at least two of the known terrorist involved in the September 11th attacks stayed in Florida. Regrettably they stayed at a beach hotel and did not attend the Super Bowl where the surveillance took place. Of course many feel that this surveillance is an invasion of privacy with the Virginia Chapter of the American Civil Liberties Union claiming that the technology is analogous to "big brother" and allows the government to trace individuals wherever they go.

So long as biometrics are fielded by local agencies without centralized control and with specific procedures that take into account privacy concerns it is highly likely that enhanced protection to national security will be marginal to none and that infringement on rights will be

greater than necessary or desired. Civil libertarians and privacy rights advocates are correct that biometrics represent a threat to individual privacy as they are now being implemented.[21] However, if implemented by the DoD as an open system solely to protect against terrorism and regulated by law, then the benefits will far outweigh any danger to individual privacy.

In short, the DoD must work with industry to ensure that its requirements are effectively incorporated into the lifecycle development of biometric applications. They must accomplish this by working hand in hand with the biometrics industry to establish industry standards to ensure inter-application communications and to preclude development of "stovepipe" applications that prohibit effective movement of data. DoD must establish a process that quickly assesses emerging biometric technology and through close coordination with the military community, the biometrics industry, and Congress develop a national identification system that protects against terrorism while ensuring individual privacy.

## THE DE FACTO U.S. IDENTIFICATION SYSTEM

You see the U.S. already has a de facto national identification system based on the Social Security Number (SSN). When established in 1935, the cards were issued with the notation "Not for Identification Purposes." This was changed in 1943 by Executive Order, which mandated that "all Federal components use the SSN exclusively when setting up new identification systems for individuals."[22] Over the years there has been no single Federal law to regulate SSN use. The result has been rabid identity theft based upon the use of a "key" that required only knowing someone else's number and a few other items of data such as name and home address. Interestingly enough this is the same information found on most state drivers licenses. Thus, with little effort a thief can easily access sensitive and critical personal information.

The use of SSNs for personal identification is currently a broken system. This is highlighted by the fact that the DoD already uses fingerprint validation to ensure that retired military pensioners that live overseas and are over 100 years of age are biometrically validated. This program dubbed Operation Mongoose operated due to a long history of overseas retirees having their identity stolen once they died and the U.S. needlessly paying benefits for decades afterwards.

The use by many states of the SSN on state drivers licenses has made that item the preferred item for individual identification. Recent history has shown that there is little to no difficulty in obtaining a driver's license under false pretenses. Thirteen of the nineteen hijackers of September 11$^{th}$ had valid driver licenses that were assumed to be "legitimate."[23] In fact,

states are now using biometrics when issuing new licenses not to catch terrorists but to catch poor drivers that have multiple private or commercial driver licenses under different names to avoid suspended driving privileges.

ECONOMICAL JUSTIFICATION FOR BIOMETRICS

Biometrics have proven themselves to be economically feasible. Commercial use of biometrics is so widespread that Mickey Mouse at Disney World already uses finger geometry to safeguard its seasonal pass program. Seasonal pass holders are registered by the geometry of their two fingers and quickly validate themselves as the individual with the season pass by placing their fingers on a sensor located in vicinity of the entry booth into Disney world. This practice precludes season pass holders from giving visiting relatives their pass during visits. In this case both Disney and the consumer benefit. Disney by reducing fraud waste and abuse and the consumer because the cost of the annual pass can be reduced due to the above costs not having to be passed back to the consumer.

The inability to properly identify citizens or individuals who are authorized medical care is having a tremendous affect on our national health care system. Estimates are that as much as 10 percent or 19 billion dollars a year is lost to Medicaid fraud and abuse. [24] It is bad when a Russian tourist receives a free liver transplant courtesy of Medicaid, but even worse, when he receives a second free liver when the first one is rejected. The total bill was a half a million dollars for the single case. [25] Nobody knows the eventual cost of the dozens of pregnant Philippine airline employees who would fly into New York or California on tourist passports and claim to be destitute thus having their delivery fees paid by the American taxpayer. It was only the size of the scam that brought it to light.[26]

A similar technology is used by customs at major international airports that are entry ports into the United States. The U.S. Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS), that operate using hand geometry, are used to bypass long immigration lines for arriving international passengers entering the United States. The booths are located in the vicinity of where passengers are validated by a customs official. Passengers with accounts simply place their palm on the sensor and validate their identity. They then pick up their bags and turn in their customs declaration form as they depart the baggage area. The process is so convenient that it is the method of choice for VIPs to include Senators and Congressmen.

Iris systems that take a photo of the details located within the colored portion of the eye are in use in a number of areas. Secured sensitive storage areas within DoD use iris scanners,

which are located at entryways and permit doors to be opened without having to make any type of physical contact with a scanner. Users position themselves within several feet of a scanner and the system finds the individual's face and eyes and validates their identity. This system like most can be used in a variety of ways. The most common type of escape from a prison is that the prisoner simply walks out by pretending to be another prisoner that has qualified for release. Conducting an iris scan prior to individuals being released from has eliminated this problem in prisons where biometric technology is used.

Despite the widespread use of biometrics, the fact that the United States lacks an effective national identification system based upon biometrics is disturbing. A major concern is that there are few laws that regulate how industry can implement identification of its customers. Before it was retracted due to protests from the American Civil Liberties Union, Dollar Rent A Car was requiring car renters to leave their thumbprint on their rental contract in an attempt to reduce vehicle theft. The aim of the "test" was to determine if leaving a fingerprint would reduce the incidence of rental cars being stolen not to make sure you're not a terrorist as some renters were informed.[27]

The military has recognized the risk of biometrics to individual privacy and was mandated by Congress to observe and respect individual privacy rights. Hence, when DNA is taken from a soldier it can only be used for identification of remains purposes. Requests to use the military DNA database for criminal or paternity purposes have been denied. Having the government responsible to ensure privacy by regulating by law how biometrics can be used rather than leaving it up to industry is paramount if individual privacy is to be protected.

## CONCLUSION

"This will remain the land of the free only so long as it is the home of the brave."

—Elmer Davis

The definition of insanity is when one does the same thing over and over and expects a different result. In these days when we find ourselves with increasing personnel tempo, increasing operations tempo and staffs that are stable or even decreasing we can no longer afford to follow that model. Army leaders must continuously assess emerging technology and be prepared to provide our military perspective and feedback to industry. The days when the Department of Defense (DoD) can dictate data ownership rights and obscure software languages for programming are over. DoD must acknowledge that we are no longer in the driver's seat in regards to the development of technology useful to the military. The commercial

sector is driving promising technology and DoD must find a way to add value in the commercial technology development process.[28] Army leaders must effectively harness technology change and either lead, follow or get out of the way.

The Department of Defense's current strategy of providing an independent military biometric capability provides critical capabilities but falls short of addressing the needs of homeland defense. From the day that the Department of Defense's Biometrics Management Office was created by public law 106-246 on July 13, 2000 the focus has been to address military needs for the biometric identification of DoD personnel rather than support to a national based identification system. The BMO is currently aligned under the Common Access Card office within the Army's Chief Information Office. Under this organization structure the BMO is ill positioned to be of service to the nation in the war against terrorism.

With the World Trade Center attack it is clear that DoD's current strategy is flawed since it provides America with no effective method of identifying its own citizens much less the terrorists that choose to hide among our population. Current executive action to require all noncitizens to use a biometric ID-Card solves only one portion of the total identification problem.

Every military commander recognizes the need to know both himself and his enemy in order to avoid peril. Today the United States cannot do either since we cannot identify our own citizens much less potential terrorists. The United States lacks even a rudimentary national identification system to preclude terrorists from operating in the open sea of what is our civilian population. America has two choices we can either remove ourselves from the global community so that we can no longer inflame terrorist or religious cults that are obsessed with us or chose to use available technology to better protect ourselves.[29]

The fact that the U.S. is reacting to terrorism can be seen throughout our America as we valiantly attempt to pour manpower into guarding our military installations, city reservoirs, schools, population and airspace. In the tradition of locking the gate once the horse is stolen we find ourselves most comfortable doing things the old fashioned way by allocating already scarce manpower against the terrorist threat that operates among us. The nation cannot afford the costs for this brute force approach nor will Americans tolerate the resulting impact to their way of life. We must change. It is no longer sufficient that we work hard; we must work both hard and smart. Biometrics is a critical tool that can be a force multiplier in our homeland defense.

There is currently a civilian uproar that the United States government failed in their mission to protect Americans by allowing a known terrorist to board a civilian airliner. Atta (one of the suspected suicide pilots) was able to live a relatively normal life in the U.S. for months after he was already identified as a wanted man and a terrorist. He obtained a driver's license,

took flight lessons, procured rental cars, traveled nationally as well as internationally and otherwise prospered in America aided by a heterogeneous identification system consisting of hundreds of stovepipe systems that cannot communicate with each other. What failed America was our lack of vision to use the tools already available to us, despite having a clear and present threat against our safety.

The most difficult issue regarding the effective use of biometrics was the inability of the biometrics industry to articulate why America needed such an accurate and timely identification system's No one was willing to pay for the cost, no matter how small, for a technology that addressed what was not determined to be a pressing requirement. Of course September 11th should have drastically changed our perspective. Having our blinds removed places us in the position of being able to fight back if we establish the correct goals. Decades ago the idea of basing intelligence systems in space or in aircraft was a source of science fiction. Today, of course, it is accepted. America can meet the challenge of terrorism to its way of life, however it must be willing think outside the box, overcome our disbelief that doing things differently will work and to use all the technology available. We cannot simple focus on using biometrics to protect DoD. The nature of terrorism is that they will seek our weak links, we must make our identification system a national system first rather than just one for the military and we must follow this up with a worldwide system.

**RECOMMENDATION**

Abraham Lincoln once said that common looking people must be the best in the world that is the reason the Lord makes so many of them. The trouble is they are difficult to tell apart, especially if they have a vested interest in remaining incognito. The world has changed; the DoD no longer has the luxury of being able to not tell its enemies from its friends. We are at war against terrorism that will stress our ability to continue the status quo.

Now is the time for the DoD to step up to the plate and to undertake the mission of a national identification system based upon biometrics. Not because it is easy or because we want the responsibility but because the security and welfare of this nation depends on the trust and dependence that only the military is in the position to provide. There is no fear of a military coup over civilian control; the DoD is the only agency that has the necessary trust of the people and the tasking by the Constitution to undertake such a task.

We can assume that the OPTEMPO of our staffs will increase while our manning, if we are lucky, will be static. We must dedicate ourselves to not only working harder but to working smarter. Thinking outside the box and making the Biometric Management Office responsible for

the implementation of a national ID system is an initial step that is best executed by placing the DoD BMO under the auspices of the Director for Homeland Defense. Failure to do so will result in our military operations becoming reactive versus proactive to enemy action.

Word count: 9349

## ENDNOTES

[1] Julian Ashbourn, "Biometrics: Advance Identity Verification" Springer, 2000.

[2] John Woodward; Katharine Webb; Elaine Newton; Milissa Bradley and David Rubenson, "Army Biometric Applications: Identifying and Addressing Social Cultural Concerns" Rand Arroyo Center, 2001.

[3] Nathan Ward, "The Fire Last Time: When terrorist first struck New York's financial district," American Heritage, December 2001.

[4] Ibid., 1.

[5] Scott Woolley, "Spotting Evil: New Technology may well be able to pick out terrorists out of a crowd and create a record of their movements-and your's too," Forbes, 15 October 2001, page 46.

[6] "History of the Fingerprint" located at web site: http://www.onin.com/fp/fphistory.html, last updated 12 April 2001.

[7] Dana Hawkins and David LaGesse, "Tech vs. Terrorists," U.S. News & World Report, October 8, 2001, pp56-57.

[8] Ibid.,2.

[9] Osamu Tsukimori, "New Tools will keep eye on flyers," The Washington Times, 8 October 2001, page A19.

[10] Ibid., 7.

[11] Ibid., 8

[12] Robert O'Harrow, "States Seek National ID Funds: Motor Vehicle Group Backs High-Tech Driver's Licenses," The Washington Post, 14 January 2002.

[13] Jabeen Bhatti, "Resort city approves using face-recognition technology," The Washington Times, 15 November 2001.

[14] James Pethokoukis, "Mass deduction: Intelligent software might scan databases for hints of terrorist attacks in the making," U.S. News and World Report, 17 December 2001.

[15] Quadrennial Defense Review Report, September 30, 2001 page 29

[16] Marco Della Cava, "Under Suspicion: Liberty could suffer was we search for the enemies within," USA Today, 24 Sept. 2001, page 1.

[17] Randall E. Stross, "Counterfeit freedom," U.S. News& World Report, October 8, 2001 page 43.

[18] Dave Boyer, "New law contains ID-card proposal" The Washington Times.

[19] Alfred Alvarez, "First to Fire: 7th FA on D-Day at Omaha Beach," Field Artillery, November-December 2001, p40.

[20] Ibid.,13.

[21] Donna Leinwand, "National ID in Development," USA Today, January 22nd 2002.

[22] Ibid.,2.

[23] Margaret Carlson, "The Case for a National ID Card: Big Brother already knows where you live. Why not let him make you safer?," Time, January 21 2001, page 52.

[24] Randy Fitzgerald, "Medicaid's Big-Time Rip-Offs," Reader's Digest, August 1999, page118.

[25] Ibid.,19.

[26] Ibid.

[27] "ACLU Protest Dollar Rent A Car fingerprinting customers," The Washington Post, Tuesday, December 4th 2001.

[28] Statement of the Honorable Jacques S. Gansler, Under Secretary of Defense Acquisition, Technology and Logistics: Hearing on Acquisition Issues, 26 April 2000.

[29] Ivan Eland, "Protecting the Homeland: The Best Defense is to Give No Offense," Cato Policy Analysis No. 306, May 5th 1998, page 8.

## BIBLIOGRAPHY

"ACLU Protest Dollar Rent A Car fingerprinting customers," The Washington Post, 4 December 2001.

Julian Ashbourn, "Biometrics: Advance Identity Verification," Springer, 2000.

Jabeen Bhatti, "Resort city approves using face-recognition technology," The Washington Times, 15 November 2001.

Dave Boyer, "New law contains ID-card proposal," The Washington Times.

Ashton Carter; John Deutch, "Catastrophic Terrorism: Tackling the New Danger," Foreign Affairs, Nov/Dec 1998, Volume 77, Number 6.

Margaret Carlson, "The Case for a National ID Card: Big Brother already knows where you live. Why not let him make you safer?," Time, 21 January 2001.

Marco Della Cava, "Under Suspicion: Liberty could suffer was we search for the enemies within," USA Today, 24 Sept. 2001.

Ivan Eland, "Protecting the Homeland: The Best Defense is to Give No Offense," Cato Policy Analysis No. 306, May 5th 1998.

Randy Fitzgerald, "Medicaid's Big-Time Rip-Offs," Reader's Digest, August 1999.

Dana Hawkins and David LaGesse, "Tech vs. Terrorists," U.S. News & World Report, October 8, 2001.

Donna Leinwand, "National ID in Development," USA Today, 22 January 2002.

Robert O'Harrow, "States Seek National ID Funds: Motor Vehicle Group Backs High-Tech Driver's Licenses," The Washington Post, 14 January 2002.

James M. Pethokoukis, "Mass deduction: Intelligent software might scan databases for hints of terrorist attacks in the making," U.S. News and World Report, 17 December 2001.

Quadrennial Defense Review Report, September 30, 2001.

Randall E. Stross, "Counterfeit freedom," U.S. News& World Report, 8 October 2001.

Statement of the Honorable Jacques S. Gansler, Under Secretary of Defense Acquisition, Technology and Logistics: Hearing on Acquisition Issues, 26 April 2000.

Osamu Tsukimori, "New Tools will keep eye on flyers," The Washington Times, 8 October 2001.

Nathan Ward, "The Fire Last Time: When terrorist first struck New York's financial district," American Heritage, December 2001.

John Woodward; Katharine Webb; Elaine Newton; Milissa Bradley and David Rubenson, "Army Biometric Applications: Identifying and Addressing Social Cultural Concerns," Rand Arroyo Center, 2001.

Scott Woolley, "Spotting Evil: New Technology may well be able to pick out terrorists out of a crowd and create a record of their movements-and your's too," Forbes, 15 October 2001.